

The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

JOHN HOLCOMB,

Defendant.

No. CR21-75-RSL

UNITED STATES' MOTION FOR
RECONSIDERATION OF
SUPPRESSION ORDER (DKT. 58)

Noted for Consideration: June 10, 2022

The Court should reconsider its order granting defendant John Holcomb's motion to suppress a video of him raping a child and two child-sex-abuse videos, which police found on Holcomb's computer in a warranted search. The Court ruled that the state warrant authorizing the search was impermissibly general. And the Court retroactively imposed a new requirement that authorization to search for digital evidence showing that a suspect controlled a computer must include a time restriction—a requirement neither the Supreme Court nor the Ninth Circuit has ever imposed. After retroactively imposing that new requirement, the Court concluded that the executing officers could not have acted in good-faith reliance on the warrant because the authorization to search for and seize evidence that Holcomb controlled the computer lacked that limitation. Dkt. 58 (Order) at 14.

The Court's conclusions miss key factual points and cannot be reconciled with binding precedent. The Court should thus reconsider its order and deny Holcomb's suppression motion.

BACKGROUND

I. The Fourth Amendment standard

The Fourth Amendment commands that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. The requirement that the warrant must sufficiently describe the place to be searched and the persons to be seized has two components. The warrant “must clearly state what is sought” (particularity). *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702 (9th Cir. 2009). And it must not be overbroad—which means that the “scope of a warrant must be limited by its probable cause” and must “‘never include more than is covered’ by that probable cause.” *United States v. King*, 985 F.3d 702, 707 (9th Cir. 2021) (citing *SDI Future Health, Inc.*, 568 F.3d at 702, and quoting *United States v. Whitney*, 633 F.2d 902, 907 (9th Cir. 1980)).

II. The Riquelme warrant

Here, the police seized a computer, laptop, and cellphone from Holcomb’s home under a valid search warrant that stated probable cause to believe that Holcomb committed the crime of second-degree rape—domestic violence against J.J. on the night of January 27, 2020. Order 2, 5 n.1. This Court found no defect in that warrant.

The police then obtained a second warrant from Skagit County Superior Court Judge Laura Riquelme authorizing a search of these digital devices. Order 3. The Court correctly concluded that the Riquelme warrant was supported by probable cause to believe that evidence that Holcomb had committed the crime of second-degree rape—domestic violence against J.J. on the night of January 27, 2020, would be found on digital devices taken from his home. Order 5–7.

The affidavit supporting the Riquelme warrant explains that when the police were executing the first warrant, they saw a security camera pointing at the bed in the bedroom where J.J. alleged that Holcomb had raped her. Order 3; Dkt. 35-1 at 52. Officers also saw surveillance footage from this camera on computer monitors. Dkt. 35-1 at 52. They later heard from Holcomb that there was video from the surveillance system of Holcomb and

1 J.J. having sex stored on the seized computer. *Id.* at 52–53. Holcomb thought there might
 2 also be a separate video on his laptop. Dkt. 35-1 at 54. And J.J. told the police that Holcomb
 3 took photos of her with his phone during sex without her consent and displayed them to
 4 her on the monitor of his computer. Order 3; Dkt. 35-1 at 49.

5 The Riquelme warrant authorized law enforcement to “enter” Holcomb’s computer,
 6 laptop, and cellphone and to “search for and seize” the “following described evidence”:

- 7
- 8 • Evidence of communications to or from [J.J.] and/or between JOHN
 9 HOLCOMB, [Jill], or [J.J.]. This communication includes but is not limited to
 10 voicemails/audio recordings, SMS, MMS, emails, chats, social media
 11 posts/online forums, contact lists and call logs from June 1, 2019 to current.
- 12 • Surveillance video or images depicting [J.J.] or JOHN HOLCOMB and any
 13 other surveillance video or images from Jan 26th 2020 to current.
- 14 • Any location data including GPS coordinates from Jan 26th 2020 to current.
- 15 • User search history from the devices to include but not limited to searched
 16 words, items, phrases, names, places, or images from Jan 26th 2020 to current.
- 17 • Files[,] artifacts or information including but not limited to, documents,
 18 photographs, videos, e-mails, social media posts, chats and internet cache that
 19 would show dominion and control for the devices.

20 Order 3.

21 The warrant says that the accompanying application (which was incorporated into
 22 the warrant) sets forth probable cause to believe that evidence related to the alleged rape
 23 “is located at” Holcomb’s seized digital devices and authorizes the police to “enter the said
 24 aforementioned other.” That awkward phrase authorized the police to “enter” the digital
 25 devices seized from Holcomb’s home to search for and seize evidence in the five categories
 26 listed in the warrant. Dkt. 41-1 at 2–3.

27 While executing the Riquelme warrant, the police discovered a black and white
 28 video showing Holcomb raping a child. Order 4; Dkt. 35-1 at 69, 75. The officer also saw
 two thumbnail images from color videos next to the child-rape video that showed “pre-

1 pubescent females . . . posed for sex.” Ex. 1.¹ He did not play either of those videos. *Id.*
 2 Instead, the police obtained a new warrant to seize all three. Order 4.

3 **III. The order suppressing Holcomb’s child-rape and sex abuse videos**

4 Holcomb challenged the Riquelme warrant on a handful of theories. This Court
 5 rejected most of them, including by specifically concluding that the Riquelme warrant was
 6 supported by probable cause.

7 But the Court still suppressed the child-rape video and the sex-abuse videos as fruits
 8 of an unlawful search. The Court held that the fifth category of evidence authorized to be
 9 seized by the warrant— “files, artifacts, or information” including “documents,
 10 photographs, videos, e-mails, social media posts, chats and internet cache” showing
 11 “dominion and control for the devices”—was insufficiently particular and authorized an
 12 overly broad search. Order 10–12. The Court then held that the police could not have relied
 13 on the warrant in good faith because this dominion-and-control provision was “so facially
 14 deficient that no executing officer could reasonably presume it to be valid.” *Id.* at 13.

15 **ARGUMENT**

16 **I. Reconsideration is proper when, as here, an order overlooks or** 17 **misapprehends facts or precedent**

18 A district court has inherent power to reconsider, modify, or rescind its interlocutory
 19 orders before entry of judgment, and may do so as long as the court retains jurisdiction
 20 over the case. *See United States v. Smith*, 389 F.3d 944, 948 (9th Cir. 2004).

21 In this district, motions for reconsideration are “disfavored” and should be brought
 22 only if a court committed a “manifest error in [its] prior ruling.” W.D. Wash. L. Crim. R.
 23 12(b)(13)(A). Manifest error includes “overlook[ing] or misapprehend[ing]” some critical
 24 legal or factual issue. W.D. Wash. L. Crim. R. 12(b)(13)(B).

25 This Court’s suppression order satisfies these standards in multiple ways, including
 26 in its Fourth Amendment analysis. But the United States requests that the Court reconsider
 27 _____

28 ¹ The motion to suppress included the first page of the report that described how the videos were discovered (Dkt.
 35-1 at 69) but omitted the second page, which is attached as Ex. 1.

only its refusal to apply the good-faith doctrine to this search. *United States v. Leon*, 468 U.S. 897, 922–25 (1984); *see United States v. Crews*, 502 F.3d 1130, 1136 (9th Cir. 2007) (a reviewing court may “proceed directly to the issue of whether there was good faith reliance” without first deciding whether a Fourth Amendment violation occurred).²

This Court should reconsider and reverse its decision on good faith. In concluding that the warrant was insufficiently particular and overbroad, the Court relied on an understanding of the Fourth Amendment’s specificity requirement that is non-obvious and arguably contrary to precedent. The Court also relied on an outdated view of the exclusionary rule that does not account for recent Supreme Court decisions. Under *Leon* and later precedents, the exclusionary rule does not apply unless the executing officers exhibited deliberate, reckless, or grossly negligent disregard for the Fourth Amendment. There was no such misconduct here.

II. Police relied in good faith on the warrant

The Court should reconsider its conclusion that the good-faith doctrine does not apply to the warranted search that uncovered Holcomb’s child-rape and sex-abuse videos.

That conclusion was incorrect. Well-trained officers would not have seen the dominion-and-control provision of the Riquelme warrant as authorizing an impermissibly general search. Indeed, this Court’s suppression order retroactively imposed a new requirement for a warrant authorizing a search for evidence that the suspect controlled a digital device being searched—a requirement that neither the Supreme Court nor the Ninth Circuit has ever imposed. On the contrary, those courts have rejected Fourth Amendment arguments like Holcomb’s, as explained below. *See, e.g., Messerschmidt v. Millender*, 565 U.S. 535, 548 (2012); *King*, 985 F.3d at 710; *United States v. Johnston*, 789 F.3d 934, 942 (9th Cir. 2015); *United States v. Schesso*, 730 F.3d 1040, 1047–51 (9th Cir. 2013); *United*

² The United States does not concede that the particularity or overbreadth aspects of the Court’s suppression order are correct. And the United States reserves its right to challenge on appeal those and any other aspects of the Court’s rulings if this motion for reconsideration is denied.

1 *States v. Giberson*, 527 F.3d 882, 887 (9th Cir. 2008), *United States v. Adjani*, 452 F.3d
2 1140, 1149–50 (9th Cir. 2006); *United States v. Hill*, 459 F.3d 966, 977–79 (9th Cir. 2006).

3 Under controlling law, the police had good reason to rely on the authorization that
4 they received from the state judge who issued this warrant. Indeed, the U.S. Department of
5 Justice continues to believe that no Fourth Amendment violation occurred here.³ And the
6 order cited no case from the Ninth Circuit or the Supreme Court that suppressed evidence
7 from a warranted search on facts comparable to these. In short, this is a quintessential good-
8 faith case. Thus, the “extreme sanction of exclusion” does not apply. *Herring v. United*
9 *States*, 555 U.S. 135, 140 (2009) (quoting *Leon*, 468 U.S. at 916).

10 **A. A reasonably well-trained officer would not have seen this warrant as**
11 **unlawful**

12 If police officers rely in good faith upon a magistrate’s decision to issue a warrant,
13 evidence obtained during a search will not be subject to suppression even if it is later
14

15 ³ As the opposition to the suppression motion explains, the United States believes that the dominion-and-control
16 provision complied with the Fourth Amendment’s specificity requirement. Dkt. 41 at 23-27. First, no date restriction
17 was required for the dominion-and-control provision because there was a fair probability that dominion-and-control
18 evidence from outside the timeframe of the alleged rape would have been useful to proving the alleged rape. The
19 provision was also as narrowly drawn by file type as possible given the nature of digital evidence. *See, e.g.,*
Giberson, 527 F.3d at 887. And it was tied to the rape allegation because evidence of dominion-and-control was
likely to be helpful in proving the authenticity of any images seized. The United States reserve the right to challenge
the court’s conclusion to the contrary in the event of an appeal.

20 The United States also believes that the court erred when it said that only the dominion-and-control
21 provision could have authorized the search that resulted in the contested videos. Order 11. As explained in the
22 opposition to the suppression motion, that search was separately authorized by the provision that allowed the
23 officers to search for and seize video of J.J. or Holcomb, even though that provision had a date restriction and the
24 video was not within it. Dkt. 41 at 12 (discussing plain view); *id.* at 23 (noting that Holcomb failed to distinguish
25 authority to search and authority to seize and explaining that this warrant allowed the police to search the specified
26 devices but limited them to seizing the five categories of data identified in the warrant). The authorization to search
27 for videos within the time frame in the warrant allowed the executing officers to look at any video that seemed
28 potentially responsive to determine whether it was. The warrant limits the search to videos “from” within the time
restriction, not videos “time stamped” within that period. Dkt. 41-1 at 3. Because timestamps are easy to alter and
unreliable, *see, e.g., Hill*, 459 F.3d at 978–79; *see also* Dkt. 59 at 9–10 (transcript of suppression hearing)
(explaining why dates on digital evidence are unreliable), any video was potentially responsive, and executing
officers were allowed to take at least a cursory look at it. That is how they found the child-rape video and the sex
abuse videos at issue. Dkt. 35-1 at 69, Ex. 1. The videos’ obvious illegality meant that the officers could lawfully
seize them under the plain-view doctrine. *Horton v. California*, 496 U.S. 128, 133 (1990) (“If an article is already in
plain view, neither its observation nor its seizure would involve any invasion of privacy.”). The videos were not the
“fruit” of any illegality. The United States also reserve the right to challenge the court’s conclusion to the contrary in
the event of an appeal.

determined that the magistrate erred in issuing the warrant. *Leon*, 468 U.S. at 922–25. While the officers’ reliance on the warrant must be “objectively reasonable,” *id.* at 922, the Supreme Court has stressed that it will be the rare case in which this standard is not met. “When officers have acted pursuant to a warrant, the prosecution should ordinarily be able to establish objective good faith without a substantial expenditure of judicial time.” *Id.* at 924.

The good-faith doctrine applies unless the officers showed “‘deliberate,’ ‘reckless,’ or ‘grossly negligent’ disregard for Fourth Amendment rights.” *Davis v. United States*, 564 U.S. 229, 238 (2011) (quoting *Herring*, 555 U.S. at 144). “The central question is ‘whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate’s authorization.’” *King*, 985 F.3d at 710 (quoting *Leon*, 468 U.S. at 922 n.23).

These principles foreclose suppression here. The Court’s conclusion that the warrant violated the Fourth Amendment turned on the lack of a temporal limit on the dominion-and-control provision. The Court held that the “lack of a temporal limitation in the Riquelme warrant’s dominion and control clause is fatal to its particularity” and that the “dominion and control clause sought materials outside the scope of probable cause due to its lack of temporal limitation.” Order 10, 11.⁴ But it was objectively reasonable for the executing officers to think that the dominion-and-control provision of the warrant was neither overbroad nor lacking in particularity even though it did not say that the evidence of dominion and control had to come from the timeframe of the alleged rape.

⁴ The Court also expressed practical doubt that dominion-and-control evidence was likely to be contested in this case. *See* Order 11 n.7. But the Court did not accept Holcomb’s argument that the police lacked probable cause to seek dominion-and-control evidence for that reason. And Holcomb’s argument is incorrect. That he did not contest ownership at the time of the search does not mean that officers lacked probable cause to search for evidence of control. Nothing would have prevented Holcomb from contesting dominion and control later, and police did not have to guess, when obtaining this warrant, about future legal arguments that Holcomb might make. Holcomb could have changed tack ahead of a trial. Even more fundamentally, the warrant’s dominion-and-control provision is not about ownership but about “dominion and *control*.” (Emphasis added.) When the magistrate signed the warrant, it was easy to imagine that Holcomb—who had just withdrawn consent to search the devices, and who was suggesting that he had been drugged on the night of the alleged rape—could argue that he did not control a device or could challenge the authenticity or completeness of a video. Additionally, the Fourth Amendment does not require the government to limit its search for evidence to evidence that is strictly necessary to proving its case.

1 No case from the Ninth Circuit or the Supreme Court says that a digital search
2 warrant's dominion-and-control provision must include a restrictive date-range limitation.
3 A date limit on such evidence would be arbitrary and unduly restrictive in many cases.
4 Imagine that a defendant used a computer during a certain period to commit a crime.
5 Evidence of dominion and control from *outside* the offense period could still be relevant
6 and important evidence to prove he had dominion and control *within* that period. An
7 electronic image of a store receipt, for example, could show that the defendant bought the
8 device before the defined period. Or a selfie photo of the defendant could show him sitting
9 at the computer and using it days after the defined period.

10 More generally, the government knows of no Supreme Court or Ninth Circuit case
11 suppressing evidence from a warranted search based on a defect in a provision authorizing
12 a search of a computer for evidence that the suspect controlled it. Given the lack of
13 precedent saying so, a reasonable officer would have had no reason to think that a
14 dominion-and-control provision like this one violated the Fourth Amendment.

15 The Supreme Court held in *Messerschmidt* that the "same standard of objective
16 reasonableness" applies to the good-faith doctrine under *Leon* and qualified immunity for
17 an officer who obtained or relied on an allegedly invalid warrant. 565 U.S. at 546 n.1. In
18 the qualified-immunity context, establishing that an officer's reliance on a warrant was
19 objectively unreasonable requires a court to identify controlling law that clearly establishes
20 that the warrant violated the Fourth Amendment.

21 In other words, the good-faith doctrine applies if the law either authorizes the
22 challenged warrant or is silent on the facts underlying a suppression motion. Thus, for
23 example, the Ninth Circuit held in *United States v. Lustig*, 830 F.3d 1075, 1082 (9th Cir.
24 2016), that good faith applied to the warrantless search of the defendant's cellphone
25 conducted before *Riley v. California*, 573 U.S. 373 (2014). The Ninth Circuit explained
26 that if "precedent had to constitute a factual match with the circumstances of the search in
27 question for the good-faith exception to apply, it would make the good-faith exception a
28 nullity because the exception would only apply when the search was necessarily

1 constitutional under existing precedent.” *Lustig*, 830 F.3d at 1082. “We decline to impose
 2 on law enforcement an obligation to constantly search for non-binding authority across all
 3 jurisdictions and to curtail their otherwise authorized activities as soon as any court casts
 4 existing precedent into doubt.” *Id.* at 1083.

5 Here, the Court’s suppression order identifies no controlling cases holding that a
 6 similar dominion-and-control provision was insufficiently specific. And in *Johnston*, a
 7 2015 case considering an analogous search provision—a provision authorizing officers to
 8 search for “items which evidence ownership or use of computer equipment found in
 9 the . . . residence”—the Ninth Circuit rejected the defendant’s argument that a search
 10 conducted under the provision constituted impermissible “rummaging” through his
 11 electronic devices. *Johnston*, 789 F.3d at 942 (rejecting a manner-of-execution challenge
 12 to the warrant). So too, the Ninth Circuit in *Schesso* specifically rejected the argument that
 13 a warrant to search the defendant’s digital devices for child pornography was overly
 14 general because it did not have date limits. 730 F.3d at 1046.⁵

15 An officer familiar with *Johnston* and *Schesso* would have been hard pressed to see
 16 that the Riquelme warrant was unlawful because its dominion-and-control provision lacked
 17 a temporal limit. Under *Messerschmidt*, that means that the executing officers here did not
 18 rely on this search warrant in deliberate, reckless, or grossly negligent disregard for the
 19 Fourth Amendment.

20 **B. It was objectively reasonable to rely on this warrant**

21 In *Messerschmidt*, the Supreme Court considered a warrant that authorized
 22 executing officers to “search for and seize *all* firearms” from a suspect’s temporary
 23 residence even though the warrant alleged that a specific black sawed-off shotgun with a
 24

25
 26 ⁵ It is a distinction without a difference that the *Schesso* warrant authorized a search for child-pornography evidence
 27 and the warrant here authorized a search for three sets of images that were evidence of rape as well as evidence that
 28 Holcomb controlled the devices being searched. Both cases involve a search for digital evidence that could have
 been anywhere on the suspect’s digital devices. And unlike the *Schesso* warrant, the warrant here *did* contain file-
 type and date limits as much as it was possible and reasonable to include them.

1 | pistol grip was used in the offense being investigated. 565 U.S. at 548. The Court held that
2 | “even if the scope of the warrant were overbroad in authorizing a search for all guns when
3 | there was information only about a specific one,” it was not “entirely unreasonable” for the
4 | officers who executed the warrant to rely on it. *Id.* The Court drew that conclusion because
5 | a magistrate judge authorized the warrant and the circumstances set out in the warrant
6 | affidavit gave rise to a fair probability that the sawed-off shotgun was not the only one that
7 | the defendant owned. *Id.*; see also *King* 985 F.3d at 710 (applying *Messerschmidt* and
8 | holding that good faith would apply even if a warrant authorizing a search for all firearms
9 | were overbroad).

10 | By analogy, even if the dominion-and-control provision in the Riquelme warrant
11 | should have included a date restriction, it was not unreasonable for the police to rely on the
12 | warrant. As in *Messerschmidt*, a judicial officer authorized the Riquelme warrant. Also, as
13 | in *Messerschmidt*, the circumstances set out in the Riquelme warrant affidavit gave rise to
14 | a “fair probability” that whether Holcomb controlled the digital devices seized from his
15 | home would help the state prove the rape allegation, even if that evidence of control was
16 | from a period before the alleged offense. *United States v. Gourde*, 440 F.3d 1065, 1066
17 | (9th Cir. 2006) (en banc) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). The good-
18 | faith doctrine therefore forecloses suppression here.

19 | The affidavit makes clear how evidence that Holcomb controlled the digital devices
20 | related to the alleged crime, so any shortcoming in the warrant in identifying that evidence
21 | was non-obvious under *Messerschmidt*. The warrant affidavit showed that digital images
22 | of J.J. and Holcomb during sex would likely be relevant to proving her allegations.
23 | Holcomb said that there would be video from the surveillance system and might be video
24 | on the laptop. Dkt. 35-1 at 52-54. And J.J. said that Holcomb took cellphone photos of her
25 | during sex and then showed them to her on his computer. *Id.* at 49.

26 | Circumstances established a fair probability that all three sets of images would help
27 | the state prove the alleged rape. And there was a fair probability that the authenticity of all
28 | three sets of images would be contested.

1 It was objectively reasonable to think that evidence that Holcomb controlled the
2 digital devices was likely to be relevant to proving both her allegations and the authenticity
3 of the images. Without evidence that Holcomb controlled the digital devices, he could have
4 argued that someone else set up the surveillance camera or edited one or more of the videos
5 to make it look incriminating. He also could have argued that he did not take photos of J.J.
6 during sex without her consent. Evidence of control was also potentially relevant if
7 investigators found video of a sexual encounter that clearly depicted J.J. but did not clearly
8 depict Holcomb.

9 Evidence that Holcomb controlled the digital devices was relevant to proving the
10 alleged rape in another way, too: J.J. alleged that Holcomb took photos of her during sex
11 without her consent and showed those photos to her while making disparaging comments
12 *right before* the alleged rape. Dkt. 35-1 at 49. Who controlled the computer and cellphone
13 was relevant to proving the photography-related allegations—allegations that prosecutors
14 could have used to prove that Holcomb coerced J.J. into the sexual encounter that occurred
15 soon after he showed her the photos. What’s more, the video and photos that Holcomb took
16 of J.J. without her consent could have been relevant to proving other crimes, including
17 under Washington State’s laws against voyeurism (RCW 9A.44.115).⁶ *See Messerschmidt*,
18 565 U.S. at 548–49 (making clear that courts can look beyond the warrant in analyzing
19 good faith). In all these ways, this warrant application “demonstrate[d] to the
20 magistrate *factually* why such a broad search and seizure authority [was] reasonable in the
21 case.” *Hill*, 459 F.3d at 975 (emphasis in original).

22 A reasonably well-trained officer could have concluded not just that there was a fair
23 probability that evidence of dominion and control would help prove the rape allegation,
24 but also that limiting the dominion-and-control evidence to the timeframe of the alleged
25 rape would have been arbitrary and unduly restrictive. Evidence of control was potentially
26 relevant to proving the allegations even if that evidence came from well before the alleged
27

28

⁶ <https://apps.leg.wa.gov/rcw/default.aspx?cite=9A.44.115>.
United States v. Holcomb, CR21-75-RSL
U.S. Mot. for Reconsideration of Suppression Order – 11

1 rape; while the timing of the rape allegations was well defined, the timing of Holcomb's
2 potentially relevant acts of control of the digital devices was not. For example, it was
3 objectively reasonable to believe that there was a fair probability that whether Holcomb
4 was the one who set up and controlled the surveillance camera filming in his bedroom
5 would be relevant to proving the rape allegation, and there was no way to know when that
6 system was set up. It was also objectively reasonable to believe that there was a fair
7 probability that evidence that Holcomb controlled the surveillance system would help the
8 state prove the rape allegations by establishing that any images taken from the computer
9 were authentic and had not been edited. After all, as the warrant affidavit states, Holcomb's
10 partner, Jill, accessed and watched a video from the surveillance system. Dkt. 35-1 at 53.
11 And the warrant affidavit explained that digital information can be altered. *Id.* at 54.

12 In short, it was objectively reasonable for the officers who sought the warrant to
13 think that there was a fair probability that dominion-and-control evidence from before the
14 period of the alleged rape would be relevant to proving the offense. That means it was also
15 objectively reasonable to believe that the Fourth Amendment allowed Judge Riquelme not
16 to restrict this warrant's dominion-and-control provision by time. From the face of this
17 warrant, the dominion-and-control provision was not obviously defective.

18 Finally, while this Court concluded that the dominion-and-control clause was overly
19 general because it lacked a time restriction, the Court's analysis of the warrant in the section
20 of the order on good faith seems to go further—the Court says that the provision also lacked
21 “relationship to crime, and file category limitations.” *Compare* Order 10–11 *with id.* at 14.
22 But these other factors were no basis for concluding that the officers did not act in good
23 faith, either.

24 It was objectively reasonable for the issuing magistrate and the executing officers
25 to believe that evidence of dominion and control had a solid tie to the crime under
26 investigation—a crime identified in the warrant itself. As just explained, evidence that
27 Holcomb controlled the computer could be relevant to showing that Holcomb took photos
28 and video of J.J. during sex. It could also be relevant to showing who had access to the

1 video on the computer. Such evidence could have been relevant to proving who made the
2 video of J.J. and Holcomb having sex, whether that video had been edited, and whether
3 Holcomb coerced J.J. with photos or video.

4 So too, it was objectively reasonable for the issuing magistrate and the investigators
5 to believe that the file-type description of the digital evidence was as precise as it could
6 have been. Evidence of control of the digital devices could have come in different but
7 difficult-to-predict forms. The provision carefully lists examples of the types of “files,
8 artifacts, or information” evidencing dominion and control that could be seized:
9 “documents, photographs, videos, e-mails, social media posts, chats and internet cache.”

10 It was thus objectively reasonable for the executing officers to believe that this
11 provision was as narrowly drawn by file type as possible, given the nature of digital
12 evidence. *See, e.g., Giberson*, 527 F.3d at 887 (“in the age of modern technology and
13 commercial availability of various forms of items, the warrant could not be expected to
14 describe with exactitude the precise form the records would take”); *Adjani*, 452 F.3d at
15 1147–48 (“Warrants which describe generic categories of items are not necessarily invalid
16 if a more precise description of the items subject to seizure is not possible.” (citation
17 omitted)); *SDI Future Health, Inc.*, 568 F.3d at 704 (when record shows that it “would have
18 been difficult to specify beforehand” which files would respond to a search, no further
19 particularity required).

20 That conclusion is made stronger by the careful limits on the four other categories
21 of evidence set out in the warrant. The Supreme Court said in *Leon* that a court determining
22 whether an officer’s reliance on a warrant was “objectively reasonable” should consider
23 “all of the circumstances.” 468 U.S. at 922 & n.23. The dominion-and-control provision
24 did not stand alone, and an officer reviewing the warrant as a whole could have reasonably
25 concluded that the judge who authorized it required file-type restrictions to the extent that
26 doing so was feasible and required under the Fourth Amendment.

C. It was also objectively reasonable to think that the video-search provision in the warrant authorized the search that resulted in the discovery of the child-rape and sex-abuse videos

A well-trained officer could also have reasonably understood that the video-search provision of the warrant authorized at least a quick look at all the videos on the digital devices that might have been responsive to the warrant. This Court implicitly recognized as much when it concluded that “a reviewing officer would need to review the lower hard drive, at least cursorily, to conclude that it did not contain surveillance videos.” Order 12 n.8. The Court’s observation matches *Andresen v. Maryland*, 427 U.S. 463, 482 (1976), which recognizes that “[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.”

The need to review, “at least cursorily,” potentially responsive videos to determine whether they came within the video-search provision means that it would have been objectively reasonable for an officer to understand the warrant to authorize at least a cursory look at any video that appeared to be responsive—even video with a timestamp from before the timeframe set out in the warrant. Contrary to the Order, the warrant did not say that the officer who searched Holcomb’s devices had to limit his search for responsive videos to digital files that were “time stamped” January 26, 2020, or later. Order 10. The warrant said that the officers could search for and seize surveillance video or images depicting J.J. or Holcomb “from” that date onward—that is, video or images *taken on* or after that date. Dkt. 41-1 at 3.

It was objectively reasonable to believe that the warrant limited the seizure based on when the video or images were taken instead of based on when they were “time stamped.” And it was also objectively reasonable to believe that a time restriction based on when the video was made satisfied the Fourth Amendment. Holcomb could have easily altered the timestamp on a video. After all, digital evidence is easy to alter, hide, destroy, disguise, or rename. *See, e.g., Hill*, 459 F.3d at 978–79 (“Computer records are extremely

1 | susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent. . . .
 2 | Criminals will do all they can to conceal contraband, including the simple expedient of
 3 | changing the names and extensions of files to disguise their content from the casual
 4 | observer. Forcing police to limit their searches to files that the suspect has labeled in a
 5 | particular way would be much like saying police may not seize a plastic bag containing a
 6 | powdery white substance if it is labeled “flour” or “talcum powder.”) (citation omitted);
 7 | *see also* Dkt. 59 at 9–10 (transcript of suppression hearing) (explaining why dates on digital
 8 | evidence are unreliable). And the warrant affidavit makes clear that Holcomb was digitally
 9 | savvy. Dkt. 35-1 at 48 (J.J. told the police that Holcomb expressed concern that there was
 10 | spyware on her phone and computer and deleted at one program from her computer and a
 11 | few apps from her phone); *id.* at 50 (Holcomb told J.J. that it was not safe to communicate
 12 | on Facebook and set up an encrypted messaging app on her phone), *id.* at 52 (Holcomb’s
 13 | computer had two monitors connected to it and an active surveillance system running and
 14 | recording, and was running iSpy64, a “known security surveillance software”). The
 15 | affidavit also explains that digital information can in many cases “still be recovered
 16 | forensically even if it had been previously deleted through the use of specialized
 17 | applications and tools available to investigators” and “can be used to corroborate or refute
 18 | the details of a suspects alibi or the statements of a victim or witness.” *Id.* at 54.

19 | It was thus objectively reasonable for the officer who found the child-rape video to
 20 | play it. He explained that he played it because it was a “black and white video file which
 21 | appeared similar to the video of Holcomb and JJ having sex.” Dkt. 35-1 at 69. When the
 22 | officer first saw a thumbnail image of it, he thought that it was “additional surveillance
 23 | video from Holcomb’s residence which is why he played it.” *Id.* Once he played it, it was
 24 | immediately obvious that it depicted criminal conduct: having sex with a prepubescent girl.
 25 | *Id.* He did not play the two other sex abuse videos but saw that “[t]he thumbnail images of
 26 | these two color video files also showed pre-pubescent females (based on their physical
 27 | development) that were posed for sex.” Ex. 1.

1 If the video and thumbnails had not been immediately and obviously recognizable
 2 as criminal during a cursory look to see whether they might be responsive to the warrant,
 3 the officer would not have been able to seize them because they were from outside the
 4 timeframe for the adult-rape videos authorized by the warrant. But because they were
 5 obviously criminal during a cursory review, the plain-view doctrine applied to them.
 6 *Horton*, 496 U.S. at 133. And in fact, the police sought and obtained a new warrant
 7 authorizing them to seize this video—more evidence of their good faith.

8 * * *

9 The record makes clear that the executing officers here did not rely on this search
 10 warrant in deliberate, reckless, or grossly negligent disregard for the Fourth Amendment.
 11 That fact ends the inquiry. Under Supreme Court and Ninth Circuit precedent, the good-
 12 faith doctrine applies.

13 **III. The Court erred by concluding that suppression was automatic in these**
 14 **circumstances**

15 In support of the conclusion that the need for deterrence was established by the
 16 Court’s overbreadth and particularity ruling, the Court cited a 1978 decision, *Mincey v.*
 17 *Arizona*, 437 U.S. 385, 393 (1978), which in turn quoted a 1969 case. Order 16. But those
 18 cases reflect an outdated view of the exclusionary rule.

19 In the 1960s and 1970s, Supreme Court decisions may indeed have “suggested wide
 20 scope for the exclusionary rule.” *Hudson*, 547 U.S. at 591. But the Supreme Court “ha[s]
 21 long since rejected that approach.” *Id.* “In time,” the Supreme Court “came to acknowledge
 22 the exclusionary rule for what it undoubtedly is—a ‘judicially created remedy’ of this
 23 Court’s own making.” *Davis*, 564 U.S. at 238.

24 “Exclusion is ‘not a personal constitutional right,’ nor is it designed to ‘redress the
 25 injury’ occasioned by an unconstitutional search.” *Id.* (citations omitted). “The rule’s sole
 26 purpose . . . is to deter future Fourth Amendment violations.” *Id.* at 236–37. And as the
 27 Supreme Court has stressed, “[r]eal deterrent value is a ‘necessary condition for exclusion,’
 28 but it is not ‘a sufficient’ one.” *Id.* at 237 (quoting *Hudson v. Michigan*, 547 U.S. 586, 596

(2006)). The Supreme Court has also repeatedly and recently instructed lower courts that any analysis of the exclusionary rule’s applicability “must also account for the ‘substantial social costs’ generated by the rule.” *Davis*, 564 U.S. at 237.

“For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs.” *Id.*; see also, e.g., *Utah v. Strieff*, 579 U.S. 232, 237 (2016) (“[T]he significant costs of this rule have led us to deem it ‘applicable only . . . where its deterrence benefits outweigh its substantial social costs.’” (quoting *Hudson*, 547 U.S. at 591)); *Herring*, 555 U.S. at 147–48 (“[T]he deterrent effect of suppression must be substantial and outweigh any harm to the justice system.”).

These principles show that the Court erred by treating suppression as an automatic consequence flowing from the Court’s conclusion that the dominion-and-control provision of the Riquelme warrant was facially deficient. That approach short-circuited the analysis required under *Leon* and other precedent.

The conclusion that a warrant was too general does not result in automatic suppression. The good-faith doctrine still applies to an overly general warrant so long as the executing officers’ reliance on the warrant does not reflect deliberate, reckless, or grossly negligent disregard for the Fourth Amendment. See, e.g., *Messerschmidt*, 565 U.S. at 548; *King*, 985 F.3d at 710 (explaining that good faith would apply even if the warrant were overbroad because “it’s plain that reasonably well-trained officers would not have known that the search of King’s residence for ‘any firearm’ was in legal doubt”). In fact, the Supreme Court has balanced the costs and benefits of suppression even for warrantless searches. See, e.g., *California v. Greenwood*, 486 U.S. 35, 44–45 (1988); *Illinois v. Krull*, 480 U.S. 340, 353 (1987).

This Court’s reasoning that the conclusion that a warrant was facially deficient ends the analysis relies in part on *United States v. Kow*, 58 F.3d 423, 428–29 (9th Cir. 1995). But the suggestion in that 27-year-old decision that the good-faith exception is unavailable to officers who rely on an overbroad warrant “absent exceptional circumstances” no longer

1 holds true. *Messerschmidt* makes clear that officers can rely on overbroad or insufficiently
2 particular warrants in good faith. *Kow* does not support suppression here.

3 This Court's suppression order did not conduct the case-specific assessment of the
4 need for deterrence that *Leon* requires. As to deterrence, the order says only that "[h]aving
5 concluded above that the dominion and control clause of the Riquelme warrant was so
6 facially deficient that no executing officer could reasonably presume it valid, the Court has
7 already determined that the deterrent purpose of the exclusionary rule would be met by
8 excluding the child pornography evidence." Order 15.

9 But the Court should have assessed whether the police's purported failure to
10 question the warrant resulted from negligence or something more, because "when police
11 mistakes are the result of negligence . . . rather than systemic error or reckless disregard of
12 constitutional requirements, any marginal deterrence does not 'pay its way.'" *Herring*, 555
13 U.S. at 147–48 (citation omitted). The Court's order moved directly from finding the
14 warrant overly general to suppression without analyzing that question.

15 There was no reckless disregard of the Fourth Amendment here. Investigators
16 obtained a warrant supported by a detailed application that this Court found established
17 probable cause. The affiant was truthful in that application; indeed, this Court saw no need
18 for a *Franks* or evidentiary hearing. This Court rightly rejected Holcomb's attacks on the
19 police. And the police consulted the prosecutor during the search. *Massachusetts v.*
20 *Sheppard*, 468 U.S. 981, 989–90 (1984). Suppression would not deter any future
21 government misconduct because this search involved no misconduct—"flagran[t]" or
22 otherwise. *Herring*, 555 U.S. at 143–44.

23 The warrant also did not reflect systemic error. Nor did the Court identify any
24 systemic error. The Court determined that the state search warrant should have specified a
25 timeframe applicable to evidence that Holcomb controlled the digital devices. Order 10–
26 11. But the Court recognized that the warrant carefully satisfied that requirement for the
27 four other categories of evidence. Especially considering the limits on the other categories
28 of evidence in this warrant, any error here was not systemic. *Cf. United States v.*

1 *McGrew*, 122 F.3d 847, 848, 850 (9th Cir. 1997) (*Leon* does not apply when a warrant fails
2 to specify “any type of criminal activity suspected or any type of evidence sought”).

3 In concluding that suppression was warranted, the Court cited a Third Circuit
4 decision for the proposition “that the balancing of deterrence against the social cost of
5 suppression is already incorporated into *Leon*’s good-faith exception.” Order 15 (citing
6 *United States v. Caesar*, 2 F.4th 160, 169 (3d Cir. 2021). But in fact, the Third Circuit
7 recognized that “[s]ince *Leon*, the Supreme Court has further refined the good faith
8 exception,” “expanded” the exception’s reach, and “further narrowed the scope of the
9 exclusionary rule.” *Caesar*, 2 F.4th at 169 (citing the Supreme Court’s decisions in *Herring*
10 and *Davis*). The Third Circuit emphasized that “[w]e do not exclude the fruits of
11 unconstitutional searches” if “any marginal deterrent benefit is outweighed by
12 [suppression’s] costs,” *id.*—the same balancing test that the United States urges the Court
13 to engage in here. And the Third Circuit ultimately “reverse[d] the District Court’s order
14 suppressing the images of child pornography and images of sexual abuse victims seized
15 from Caesar’s electronic devices.” *Id.* at 180.

16 Precedent likewise forecloses suppression here. In *Davis*, the Supreme Court made
17 clear that it had “abandoned the old, ‘reflexive’ application of the [exclusionary rule], and
18 imposed a more rigorous weighing of its costs and deterrence benefits.” *Id.* What’s more,
19 the Supreme Court “recalibrated [the] cost-benefit analysis in exclusion cases to focus the
20 inquiry on the ‘flagrancy of the police misconduct’ at issue.” *Id.* (citation omitted). Here,
21 the technical and non-flagrant nature of any deficiency in this warranted search carries little
22 weight in the exclusionary rule’s required cost-benefit analysis. On the other side of the
23 scale, of course, the social costs of suppressing the evidence against Holcomb are
24 enormous: If the suppression order stands, this child rapist will walk free.

25 CONCLUSION

26 The executing officers engaged in no misconduct here. This Court faulted a state
27 court for how it wrote one provision of a detailed search warrant that included many
28 carefully drawn restrictions. But the technical defect identified by this Court did not justify

1 suppression. This is not a close case: “the extreme sanction of exclusion is inappropriate.”
2 *Leon*, 468 U.S. at 926; *see Herring* 555 U.S. at 140. The Court should therefore vacate its
3 prior order (Dkt. 58) and deny Holcomb’s suppression motion.

4 June 10, 2022.

5 Respectfully submitted,

6 NICHOLAS W. BROWN
7 United States Attorney

8 s/ Teal Luthy Miller

9 TEAL LUTHY MILLER
10 MATTHEW P. HAMPTON
11 JONAS LERMAN
12 Assistant United States Attorneys
13 LAURA HARMON
14 Special Assistant United States Attorney
15 700 Stewart Street, Suite 5220
16 Seattle, WA 98101-1271
17 (206) 553-7970
18 teal.miller@usdoj.gov
19 matthew.hampton@usdoj.gov
20 jonas.lerman@usdoj.gov
21 laura.harmon@usdoj.gov
22
23
24
25
26
27
28